Project: implement the Rho method of reduced SM3

--寻找到碰撞的位数：前 10 位

代码说明：套用之前写的 sm3 算法，然后利用 Rho 攻击构造简化版 sm3（取前 10 位）碰撞，具体思路为对一个输入的随机数进行简化 sm3 算法，得到的输出值再进行简化 sm3 算法，其中 一条线为一次只进行一次 sm3，另一条线为一次进行两次 sm3，然后每次都比较这两条线的值是否相等，如果发现相等，则寻找到碰撞，而且同时寻找到其构成的环：即为第二条线进行的 sm3 次数减第一条线进行的 sm3 次数

运行指导：直接运行 py 文件

运行结果截图：